REMARKS

The Office Action of January 25, 2006, has been received and its contents carefully reviewed. By the above Amendment, Applicants have amended claims 1, 2, 37, 38 and 73 to more distinctly highlight the features of the present invention. Claims 1-75 remain pending in the application. No new matter is introduced by this Amendment. Thus, Applicants respectfully submit that no new matter is presented by entry of this Amendment and that the application is in condition for allowance.

The rejection of claims 1-72 based on U.S. Patent No. 6,816,596 to *Peinado et al.* is respectfully overcome, because *Peinado et al.* fails to disclose, teach or suggest all of the features recited in the pending claims. For example, independent claim 1, as amended (emphasis added), recites:

> A system for distributing digital documents having usage rights associated therewith, said system comprising:
> a server having at least one digital document stored thereon;
> a client computer having a standard application program including a rendering engine capable of being accessed to render content;
> a communications network coupled to said client and said server; and
> a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions for accessing the rendering engine,
> **wherein the security module intercepts requests to the rendering engine that would enact a violation of usage rights associated with the content**; and

independent claim 37, as amended (emphasis added), recites:

> A method for distributing digital documents having usage rights associated therewith, said method comprising:
> storing at least one digital document on a server;
> requesting, over a communications network, the at least one digital document from a client computer having a standard application program including a rendering engine capable of being accessed to render content; and
> enforcing security conditions for accessing the rendering engine with a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions,
> **wherein the security module intercepts requests to the rendering engine that would enact a violation of usage rights associated with the content.**

Thus, independent claims 1, and 37, as amended, include the novel features of a security module which is downloaded to and included in a client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions, and wherein the security module intercepts requests to a rendering engine that would enact a violation of usage rights associated with content.

By contrast, *Peinado et al.* is directed to a conventional DRM system where content is encrypted and transmitted to a client device. The user of the client device requests access to the content and before decryption can occur a license with usage rules and permission must be acquired. The process of acquiring the license involves a secure client device black box with a private/public key pair and a license issuing service authenticating the black box before a license is issued. After the license is issued, the DRM system validates that the rendering engine is collaborative with the DRM system and that the rendering engine is trusted. Assuming that license is valid and any terms are met, the rendering engine is designed to run with the DRM system, and the content is decrypted and released to the rendering engine, as described below (see, e.g., col. 34, lines 42-59 of *Peinado et al.*).

> As was set forth above, when the rendering application **34** sends digital content **12** to the black box **30** for decryption, the black box **30** and/or the DRM system **32** preferably authenticates that such rendering application **34** is in fact the same rendering application **34** that initially requested the DRM system **32** to run (step **531** of FIG. **5**) and that the rendering application **34** itself satisfies any relevant terms in the corresponding digital license **16**. In addition, such authentication ensures that such rendering application **34** can be trusted to handle the decrypted or 'naked' digital content **12** in an appropriate manner, and also that the rendering application **34** can be trusted to handle other sensitive matter (i.e., keys, encrypted matter, and/or other trusted matter). However, and referring now to FIG. **13**, it is to be recognized that the digital content **12** likely will 'flow' in a path **58** from the rendering application **34** to an ultimate destination **60** by way of one or more modules **62** that define such path **58**.

By contrast, in the invention recited in independent claims 1, and 37, the rendering engine does not have to collaborate with the DRM system, i.e., the rendering engine need not be aware that the DRM system is present. For example, this can be accomplished by the DRM system "wrapping" the rendering engine and wherein the security module intercepts requests to the rendering engine that would enact a violation of usage rights associated with the content. In other words, the DRM system retains control of the use of the content instead of relying on the rendering engine having to cooperate with the DRM system, as further described below (see, e.g., paragraph [0053] of Applicants' published patent application).

> **[0053]** Connection module **236** can be a client side software component which verifies the integrity of the environment of client **230** by verifying that UI module **234** is attached to browser **232**, identifies the user of client **230**, i.e. the person requesting content, retrieves the document and the appropriate list of rights sent by rights management module **224**, and in appropriate circumstances, unencrypts any retrieved documents that are encrypted and generates any necessary signatures and/or keys. UI module **234** can be a client side component that monitors requests from the user to access content of documents **222** and either grants or denies the request based on the list of rights retrieved by connection module **236**. Further, UI module **234** can disable
>
> specified functions of browser **232** and the operating system of client **230** based on the list of rights in the manner described below, by interfacing with the operating system API and intercepting and redirecting commands for example. Connection module **236** verifies that the industry standard rendering engine running in the environment of client **230** has not been tampered with or otherwise compromised in a way that may allow the user to access protected content in a way that bypasses UI module **234**.

Accordingly, Applicants respectfully submit that independent claims 1 and 37, as amended, are allowable over *Peinado et al.* Dependent claims 2-36 and 38-72 are allowable over *Peinado et al.* on their own merits and for at least the reasons as argued above with respect to their independent claims.

The rejection of claims 73-75 based on U.S. Patent No. 6,311,269 to *Luckenbaugh et al.* is respectfully overcome, because *Luckenbaugh et al.* fails to disclose, teach or suggest all of the features recited in the pending claims. For example, independent claim 73, as amended (emphasis added), recites:

> An HTML document adapted to be rendered by Web browser in a secure environment, said document comprising:
> an HTML header defined between header tags;
> an HTML body containing content; and
> **security information embedded in said header, said security information being associated with one or more usage rights for the content,**
> **wherein the HTML header, the HTML body, and the security information are delivered to a client computing system, and**
> **the client computing system interprets the security information and honors the usage rights while processing the HTML body and the HTML header.**

Thus, independent claim 73, as amended, includes the novel features of an HTML header, HTML body, and security information that are delivered to a client computing system, wherein the client computing system interprets the security information and honors usage rights

for content and associated with the security information while processing the HTML body and the HTML header.

By contrast, the system of *Luckenbaugh et al.* does not transmit governed content to a client computer. Specifically, as described below (see, e.g., col. 10, 37-49), *Luckenbaugh et al.* is directed to a system that explicitly filters material before it arrives at a client system and based on (i) a cookie stored on a client computer that is built based on authentication information of the user, and (ii) HTML tags in the content from a standard web server.

> This invocation of GETPAGE detects the existence of the cookie value within dynamic mappings, and can thus infer that the user has already performed the authentication process, through the fact that the browser is capable of supplying a valid known cookie value. GETPAGE thus retrieves the credentials information from the mappings (413), retrieves the HTML file specified in the URL, filtering it in accordance with whether the user's credentials are sufficient to be allowed access to the HTML page, or any fine-grained portion thereof, and adding other items to the HTML such as images and headers, and returns this filtered reply back to the browser (414), as will now be discussed in detail.

Accordingly, the system of *Luckenbaugh et al.* includes in relevant part (A) a client system with standard browser, (B) a security server, and (C) a Web server with standard web server system. The *Luckenbaugh et al.* system has A request content from B. B then forwards the request to C. C generates the response with tags that identify security levels of the information contained in the response (web pages). B authenticates the user of A and stores the authentication information in A as a cookie. B looks up what security level the user of A has. B then examines the response from C and looks for security tags and eliminates content this is not of the proper security level. However, this fails to disclose teach or suggest the novel features of an HTML header, HTML body, and security information that are delivered to a client computing system, wherein **the client computing system** interprets the security information and honors **usage rights for content** and associated with the security information while processing the HTML body and the HTML header, as required by independent claim 73, as amended.

The present Office Action further relies on Figure 2B, steps 233 and 234, of *Luckenbaugh et al.* However, the noted steps merely disclose using cookies as part of authentication steps of a user, but not with respect to usage rights for content.

Accordingly, Applicants respectfully submit that independent claim 73, as amended, is allowable over *Luckenbaugh et al.* Dependent claims 74-75 are allowable over *Luckenbaugh et al.* on their own merits and for at least the reasons as argued above with respect to their independent claims.

Further, the present invention recited in independent claims 1, 37 and 73 includes recognition of problems discovered with respect to conventional digital rights management (DRM) systems, for example, as described at page 2 of Applicants' Published Application:

> **[0014]** The second approach is to utilize proprietary formats wherein the document can only be rendered by a select rendering engine that is obligated to enforce the publisher's rights. Of course, this approach requires the use of a single proprietary format and loses the ability to combine plural popular formats and the richness of content associated therewith. Further, this approach requires the user to use a proprietary rendering application that must be obtained and installed on the user's computer and requires development of the rendering application for each format to be rendered in a secure manner. Further, the documents must be generated or converted using non-standard tools.

The present invention recited in independent claims 1, 37 and 73, advantageously, addresses the discovered problems with respect to conventional DRM systems, for example, as described at page 6 of Applicants' Published Application:

> **[0063]** The preferred embodiment utilizes a standard rendering engine of an application program, such as a browser, a word processor, or any other application or display program. The preferred embodiment achieves this by interfacing with the application and standing between the application and the document to control access to the document. Accordingly, a separate proprietary rendering engine for each document format is not required. Further, any data format supported by the application will be supposed by the invention without modification. It can be seen that the preferred embodiment permits DRM systems to be adapted to standards, such as TCP/IP and the use of browsers to render HTML. Further, the preferred embodiment facilitates various functionality that permits DRM to be applied to systems in a manner that is transparent to the user. Several examples of methods of operation of document distribution system **200** are described below.

By contrast, *Peinado et al.* and *Luckenbaugh et al.*, alone or in combination, fail to disclose, teach or suggest the noted features recited in independent claims 1, 37 and 73, nor recognize or address the discovered problems with conventional DRM systems. Accordingly, one of ordinary skill in the art would find no motivation to arrive at the invention recited in independent claims 1, 37 and 73, based on *Peinado et al.* and *Luckenbaugh et al.*, alone or in combination, absent improper hindsight reconstructions of Applicants' invention based on Applicants' disclosure.

The present amendment is submitted in accordance with the provisions of 37 C.F.R. §1.116, which after Final Rejection permits entry of amendments placing the claims in better form for consideration on appeal. As the present amendment is believed to overcome outstanding rejections under 35 U.S.C. § 102, the present amendment places the application in better form for consideration on appeal. It is therefore respectfully requested that 37 C.F.R. §1.116 be liberally construed, and that the present amendment be entered.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,

NIXON PEABODY, LLP

/Carlos R. Villamar, Reg. # 43,224/
Carlos R. Villamar
Reg. No. 43,224

NIXON PEABODY LLP
CUSTOMER NO.: 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080